

WHAT IS CLAIMED IS:

1 1. A basic input/output system (BIOS) update file
2 comprising:
3 a signed data area including a volume header, signed
4 data, and executable update code;
5 a signature; and
6 an unsigned data area including an update command
7 list and unsigned data.

1 2. The BIOS update file of claim 1 further comprising a
2 file header.

1 3. The BIOS update file of claim 2 in which the file
2 header comprises data in conformance with an extensible
3 firmware interface (EFI) specification.

1 4. The BIOS update file of claim 1 in which the volume
2 header comprises a list representing locations of components
3 within the BIOS update file.

1 5. The BIOS update file of claim 1 in which the signed
2 data area comprises:
3 secure BIOS update data; and
4 an access control list representing permitted
5 commands.

1 6. The BIOS update file of claim 1 in which the
2 executable update code comprises code to enforce security
3 rules regarding types of modifications permitted to the signed
4 data area.

1 7. The BIOS update file of claim 1 in which the update
2 command list comprises commands requested by an
3 unauthenticated entity for modifications of the signed data.

1 8. A method comprising;
2 executing update code in a basic input/output system
3 (BIOS) update file to modify data in an unsigned data portion
4 and add commands relating to the data;
5 verifying a digital signature of the BIOS update
6 file;
7 executing the update code for processing the
8 commands in the unsigned data portion affecting data in a
9 signed data portion; and
10 committing the BIOS update file.

1 9. The method of claim 8 in which the unsigned data
2 portion comprises unauthenticated data.

1 10. The method of claim 8 in which verifying comprising
2 aborting upon occurrence of verification failure.

1 11. The method of claim 8 in which executing the update
2 code for processing the commands comprises:
3 verifying the commands against an access control
4 list; and
5 in response to the verifying, modifying the signed data
6 portion with the data in the unsigned data portion.

1 12. A computer program product, tangibly embodied in an
2 information carrier, for updating a flash memory basic
3 input/output system (BIOS), the computer program product being
4 operable to cause data processing apparatus to:
5 execute update code in a BIOS update file to modify data
6 in an unsigned data portion and add commands relating to the
7 data;
8 verify a digital signature of the BIOS update file;

9 execute the update code for processing commands in the
10 unsigned data portion affecting data in a signed data portion;
11 and
12 commit the BIOS update file.

1 13. The product of claim 12 in which the unsigned data
2 portion comprises unauthenticated data.

1 14. The product of claim 12 in which verifying comprises
2 aborting upon occurrence of verification failure.

1 15. The product of claim 12 in which executing the
2 update code for processing commands causes the data processing
3 apparatus to:

4 verify the commands against an access control list; and
5 in response to the verifying, modify the signed data
6 portion with the unsigned data portion.

1 16. A method comprising:

2 adding data to an unsigned data portion of a basic
3 input/output system (BIOS) update file;

4 adding commands to the unsigned data portion of the BIOS
5 update file;

6 verifying a signature in the BIOS update file with a
7 signature residing in target hardware;

8 verifying the commands against an access control list
9 residing in a signed data portion of the BIOS update file; and

10 modifying data in the signed data portion of the BIOS
11 update file with data in the unsigned portion in response to
12 the commands.

1 17. The method of claim 16 in which the commands
2 comprise:

3 a command to add data in the unsigned data portion to
4 data in the signed data portion;
5 a command to modify data in the signed data portion with
6 data in the unsigned data portion; and
7 a command to delete data in the signed data portion.

1 18. The method of claim 16 in which verifying the
2 signature in the BIOS update file with the signature in the
3 target hardware comprises a public key/private key encryption
4 process.

1 19. The method of claim 18 in which the public
2 key/private key encryption process is an RSA encryption
3 process.

1 20. The method of claim 16 further comprising generating
2 an image for the data in the signed data portion.

1 21. The method of claim 20 further comprising flashing
2 the image into flash memory of target hardware.

1 22. The method of claim 21 in which the flash memory
2 comprises flash memory modules.

1 23. A computer program product, tangibly embodied in an
2 information carrier, the computer program product being
3 operable to cause data processing apparatus to:
4 add data to an unsigned data portion of a basic
5 input/output system (BIOS) update file;
6 add commands to the unsigned data portion;
7 verify a signature in the BIOS update file with a
8 signature in target hardware;
9 verify the commands against an access control list (ACL)
10 residing in a signed portion of the BIOS update file; and

11 modify data in the signed portion with data in the signed
12 portion in response to the commands.

1 24. The product of claim 23 in which the commands
2 comprise:

3 a command to add data from the unsigned data portion to
4 data in the signed data portion;

5 a command to modify data in the signed data portion with
6 data in the unsigned data portion; and

7 a command to delete data in the signed data portion.

1 25. The product of claim 23 further causing the
2 processor to:

3 generate an image for the data in the signed data
4 portion.

1 26. The product of claim 25 further causing the
2 processor to:

3 flash the image into a flash memory pf the target
4 hardware.

1 27. A system comprising:

2 a processor;

3 a memory including a basic input/output system (BIOS)
4 installation process, and a flash memory containing a BIOS
5 with digital signature verification;

6 a medium containing a BIOS update file, the BIOS update
7 file comprising:

8 a signed data portion including a volume header, signed
9 data and executable update code to configure the signed data
10 with unsigned data in an unsigned data portion; and
11 a digital signature.

1 28. The system of claim 27 in which the BIOS update file
2 further comprise:

3 an access control list having authorized commands in the
4 signed data portion; and

5 a list of commands in unsigned data portion.

1 29. The system of claim 28 in which the authorized
2 commands comprise commands to enforce security rules regarding
3 types of modifications permitted to the signed data.